digital certificate and public key
Terms used: digital certificate public key

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Open results in a new window
Refine these results with
Try this search in The A

Results 1 - 20 of 1,266 Result page: 1 2 3 4 5 6 7 8 9 10 next >>

1 Public key superstructure "it's PKI Jim, but not as we know it!"
Stephen Wilson
March 2008 IDtrust '08: Proceedings of the 7th symposium on Identity and trust on the Internet
Publisher: ACM
Full text available: Pdf (684.07 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 32, Downloads (12 Months): 84, Citation Count: 0

While PKI has had its difficulties (like most new technologies) the unique value of public key authentication in paperless transactions is now widely acknowledged. The naïve early vision of a single all-purpose identity system has given way to a ...

Keywords: PKI, authentication, digital certificates, public key infrastructure

2 Teaching secure communication protocols using a game representation
Leonard G. C. Hamey
January 2003 ACE '03: Proceedings of the fifth Australasian conference on Computing education - Volume 20, Volume 20
Publisher: Australian Computer Society, Inc.
Full text available: Pdf (252.19 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 103, Citation Count: 1

The Security Protocol Game is a highly visual and interactive game for teaching secure data communication protocols. Students use the game to simulate protocols and explore possible attacks against them. The power of the game lies in the representation ...

Keywords: PGP, blind signature, computer network, cryptography, digital signature, key exchange, man-in-the-middle attack, protocols, replay attack, secure communication

3 A secure infrastructure for service discovery and access in pervasive computing
Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, Anupam Joshi
April 2003 Mobile Networks and Applications, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: Pdf (308.34 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 137, Citation Count: 9

Security is paramount to the success of pervasive computing environments. The system

presented in this paper provides a communications and security infrastructure that goes far in advancing the goal of anywhere-anytime computing. Our work securely enables ...

Keywords: distributed services, extensible markup language, pervasive computing, security, smartcards

4 Pseudonym management using mediated identity-based cryptography
Thibault Candebat, Cameron Ross Dunne, David T. Gray
November 2005 DIM '05: Proceedings of the 2005 workshop on Digital identity management
Publisher: ACM
Full text available: Pdf (293.16 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 94, Citation Count: 1

Mobile Location-Based Services (LBS) have raised privacy concerns amongst mobile phone users who may need to supply their identity and location information to untrustworthy third parties in order to access these applications. Widespread acceptance of ...

Keywords: SEM architecture, identity-based encryption, location-based services, pseudonymity

5 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration
Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 Mobile Networks and Applications, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: Pdf (107.24 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 196, Citation Count: 1

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, ...

Keywords: PKIs, PLMNs, asymmetric cryptography

6 Wireless authentication using remote passwords
Andrew Harding, Timothy W. van der Horst, Kent E. Seamons
March 2008 WiSec '08: Proceedings of the first ACM conference on Wireless network security
Publisher: ACM
Full text available: Pdf (184.23 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 34, Downloads (12 Months): 148, Citation Count: 0

Current wireless authentication mechanisms typically rely on inflexible shared secrets or a heavyweight public-key infrastructure with user-specific digital certificates and, as such, lack general support for environments with dynamic user bases where ...

Keywords: SAW, SRP, decentralized wireless authentication

7 A semantics for web services authentication
Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon
January 2004 POPL '04: Proceedings of the 31st ACM SIGPLAN-SIGACT symposium on Principles of

programming languages
Publisher: ACM
Full text available: Pdf (234.06 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 22, Downloads (12 Months): 169, Citation Count: 8

We consider the problem of specifying and verifying cryptographic security protocols for XML web services. The security specification WS-Security describes a range of XML security tokens, such as username tokens, public-key certificates, and digital ...

Keywords: XML security, applied pi calculus, web services

8 A semantics for web services authentication
Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon
January 2004 ACM SIGPLAN Notices, Volume 39 Issue 1
Publisher: ACM
Full text available: Pdf (234.06 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 22, Downloads (12 Months): 169, Citation Count: 8

We consider the problem of specifying and verifying cryptographic security protocols for XML web services. The security specification WS-Security describes a range of XML security tokens, such as username tokens, public-key certificates, and digital ...

Keywords: XML security, applied pi calculus, web services

9 An authentication framework for hierarchical ad hoc sensor networks
Mathias Bohge, Wade Trappe
September 2003 WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security
Publisher: ACM
Full text available: Pdf (263.78 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 17, Downloads (12 Months): 179, Citation Count: 4

Recent results indicate scalability problems for flat ad hoc networks. To address the issue of scalability, self-organizing hierarchical ad hoc architectures are being investigated. In this paper we explore the task of providing data and entity authentication ...

Keywords: TESLA, ad hoc networks, authentication, handoff

10 Certificateless signcryption
M. Barbosa, P. Farshim
March 2008 ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security
Publisher: ACM
Full text available: Pdf (216.69 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 21, Downloads (12 Months): 85, Citation Count: 0

Certificateless cryptography inherits a solution to the certificate management problem in public-key encryption from identity-based techniques, whilst removing the secret key escrow functionality inherent to the identity-based setting. Signcryption schemes ...

Keywords: certificateless, insider security, signcryption

11 Dynamic pharming attacks and locked same-origin policies for web browsers
Chris Karlof, Umesh Shankar, J. D. Tygar, David Wagner
October 2007 CCS '07: Proceedings of the 14th ACM conference on Computer and communications security
Publisher: ACM
Full text available: Pdf (504.43 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 124, Downloads (12 Months): 684, Citation Count: 2

We describe a new attack against web authentication, which we call *dynamic pharming*. Dynamic pharming works by hijacking DNS and sending the victim's browser malicious Javascript, which then exploits DNS rebinding vulnerabilities and the name-based ...

Keywords: pharming, same-origin policy, web authentication

12 Developing a security protocol for a distributed decision support system in a healthcare environment
Liang Xiao, Paul Lewis, Alex Gibb
May 2008 ICSE '08: Proceedings of the 30th international conference on Software engineering
Publisher: ACM
Full text available: Pdf (1.30 MB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 37, Downloads (12 Months): 134, Citation Count: 0

In this paper, we describe the unique security issues involved in healthcare domains. These have been addressed to the needs of the HealthAgents project. In the proposed approach, several levels of security have been provided in accordance with Software ...

Keywords: distributed decision support system, healthcare, security model

13 Analysis of the SPV secure routing protocol: weaknesses and lessons
Barath Raghavan, Saurabh Panjwani, Anton Mityagin
March 2007 ACM SIGCOMM Computer Communication Review, Volume 37 Issue 2
Publisher: ACM
Full text available: Pdf (369.47 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 82, Citation Count: 0

We analyze a secure routing protocol, Secure Path Vector (SPV), proposed in SIGCOMM 2004. SPV aims to provide authenticity for route announcements in the Border Gateway Protocol (BGP) using an efficient alternative to ordinary digital signatures, called ...

Keywords: BGP, routing, secure path vector

14 Early adopters an internet 2 middleware project
Jay Graham, Jeffrey Cepull
October 2000 SIGUCCS '00: Proceedings of the 28th annual ACM SIGUCCS conference on User services: Building the future
Publisher: ACM
Full text available: Pdf (156.42 KB) Additional Information: full citation, references, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 23, Citation Count: 0

Keywords: EDUPerson, IMS, LDAP, interoperability, middleware

15 Phishing attacks and solutions
Mohamad Badra, Samer El-Sawda, Ibrahim Hajjeh
August 2007 MobiMedia '07: Proceedings of the 3rd international conference on Mobile multimedia communications
Publisher: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)
Full text available: Pdf (199.92 KB) Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): 92, Downloads (12 Months): 148, Citation Count: 0

Phishing is a form of online identity theft employing both social engineering and technical subterfuge to steal user credentials such as usernames and passwords. Targeted data sources include especially Web pages, email spam, domain names. Mounting a ...

Keywords: Diffie-Hellman, RSA, SRP, TLS, phishing, public key infrastructures

16 The PERMIS X.509 role based privilege management infrastructure
David W. Chadwick, Alexander Otenko
June 2002 SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies
Publisher: ACM
Full text available: Pdf (180.46 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 51, Citation Count: 12

This paper describes the output of the PERMIS project, which has developed a role based access control infrastructure that uses X.509 attribute certificates (ACs) to store the users' roles. All access control decisions are driven by an authorization ...

Keywords: Privilege management infrastructure, RBAC, X.509, XML, attribute certificates, authorization, policies

17 Securing user inputs for the web
Jan Camenisch, abhi shelat, Dieter Sommer, Roger Zimmermann
November 2006 DIM '06: Proceedings of the second ACM workshop on Digital identity management
Publisher: ACM
Full text available: Pdf (655.02 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 64, Downloads (12 Months): 265, Citation Count: 0

The goal of this paper is to study *secure and usable* methods for providing user input to a website. Three principles define security for us: certification, awareness, and privacy. Four principles define usability: contextual awareness, semantic ...

Keywords: user interface designs

18 User centricity: a taxonomy and open issues
Abhilasha Bhargav-Spantzel, Jan Camenisch, Thomas Gross, Dieter Sommer
November 2006 DIM '06: Proceedings of the second ACM workshop on Digital identity management
Publisher: ACM
Full text available: Pdf (128.75 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 221, Citation Count: 0

User centricity is a significant concept in federated identity management (FIM), as it provides to stronger user control and privacy. However, several notions of user-centricity in the FIM

community render its semantics unclear and hamper future research ...

Keywords: delegation, identity management systems, privacy, security, taxonomy, user centric, user control

19 Coercion-resistant electronic elections

Ari Juels, Dario Catalano, Markus Jakobsson
November 2005 WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society
Publisher: ACM
Full text available: Pdf (165.24 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 99, Citation Count: 2

We introduce a model for electronic election schemes that involves a more powerful adversary than previous work. In particular, we allow the adversary to demand of coerced voters that they vote in a particular manner, abstain from voting, or even disclose ...

Keywords: coercion-resistance, electronic voting, mix networks, receipt-freeness

20 Public infrastructures for internet access in metropolitan areas

Elias C. Efstathiou, Fotios A. Elianos, Pantelis A. Frangoudis, Vasileios P. Kemerlis, Dimitrios C. Paraskevaidis, Eleftherios C. Stefanis, George C. Polyzos
September 2006 AcessNets '06: Proceedings of the 1st international conference on Access networks
Publisher: ACM
Full text available: Pdf (129.47 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 106, Citation Count: 0

Wireless Community Networks (WCNs) are metropolitan-area networks with nodes owned and managed by volunteers. These networks can be used to build large scale public infrastructures for providing ubiquitous wireless broadband access through the private ...

Keywords: WiFi networks, community networks, incentives, peer-to-peer, secure VoIP, security